Namespace Management for Personal Identity Verification (PIV) Applications and Data Objects

Special Publication 800-73 Supplementary Information

October 6, 2005

1. Introduction

The Personal Identity Verification (PIV) framework established by Federal Information Processing Standards Publication 201 includes an on-card application called the PIV Card Application and a number of data objects that represent PIV credential elements. These data objects are stored on PIV smart cards for use in identity verification processes, and collectively comprise the PIV data model. The PIV data model is specified in NIST Special Publication 800-73, Appendix A.

The PIV Card Application and each of the PIV data objects are provided with unique names from controlled and managed sets of names called *namespaces*. There are four namespaces defined in SP800-73:

- Registered Identifier (RID) namespace for labeling PIV card applications

- Object Identifier (OID) namespace for addressing PIV data objects at the Client Applications Programming Interface

- BER-TLV tag namespace for addressing PIV data objects at the Card Command Interface

- Key References

These namespaces are controlled and managed to assure interoperability of PIV cards across all PIV programs.

As new data objects are added to the PIV data model, they will be provided unique names in accordance with the PIV namespace management scheme described herein. The National Institute of Standards and Technology (NIST) is responsible for implementing and operating this scheme. Since PIV credential objects are the foundation of the PIV framework, it is expected that new credential objects will only be created in the process of updating FIPS 201 and associated Special Publications. Data objects and card applications that are not part of the PIV application domain may be added to PIV cards, but naming schemes for these applications and data objects are outside the scope of PIV namespace management.

It should be noted that the card and client interfaces defined in SP800-73 do not support retrieval of sub-elements of these PIV data objects. This *Technical Note* therefore does not address management of the tag values associated with these sub-elements.

2. Registered Identifier for PIV Card Applications

Card applications are referenced by an Application Identifier (AID) in accordance with International Standard ISO 7816 Part 5. This AID consists of a Registered Identifier (RID) unique to the application domain, and a Proprietary Extension (PIX). The RID for the PIV application domain is ‘A0 00 00 03 08’. This RID as been assigned and registered to NIST.

The PIX portion of the AID of the PIV Card Application consists of the PIV Card Application indicator ’00 00 10 00’ and two version bytes ’01 00’.

The complete AID for the PIV Card Application described in the April 8, 2005 version of SP800-73 is therefore:

‘A0 00 00 03 08 00 00 10 00 01 00’

NIST will update and publish subsequent versions of the PIV Card Application AID as required to synchronize it with future revisions of SP800-73. NIST will also provide AIDs for other card applications in the PIV application domain.

3. Object Identifiers for PIV Data Objects

PIV data objects are referenced by Object Identifiers at the Client Application Programming Interface (API). These OIDs are taken from the PIV arc of the NIST Computer Security Object Register (http://csrc.nist.gov/csor/) and are of the form 2.16.840.1.101.3.7.X.Y.Z. The value of X is 2 for all PIV data objects except the Card Capability Container. The Card Capability Container data object is a direct carryover from the earlier Government Smart Card Interoperability Specification, Version 2.1 (NISTIR 6887) and the value of X is 1 for this object.

The Y and Z values of PIV data objects are the decimal representation of the two byte hexadecimal GSC-IS Container identifiers in SP800-73 Table 1. For example, the two byte identifier for the Facial Image Buffer in Table 1 is 0x6030, and the PIV OID for this object is therefore 2.16.840.1.101.3.7.2.96.48.

NIST will use this scheme to construct OIDs for new PIV credential element objects as these objects are created.

4. ASN.1 Tags for PIV Data Objects

4.1 BER-TLV Tag Encoding

The initial release of SP 800-73 uses two-byte BER-TLV tags for the PIV data objects. Two-byte tags were chosen because most one-byte tags already have meaning in the context of an integrated circuit card and the use of two-byte tags provides a uniform and linear namespace with room to grow in a uniform and linear way in the future.

A two-byte BER-TLV tag value is encoded as three bytes as shown in Figure 1.

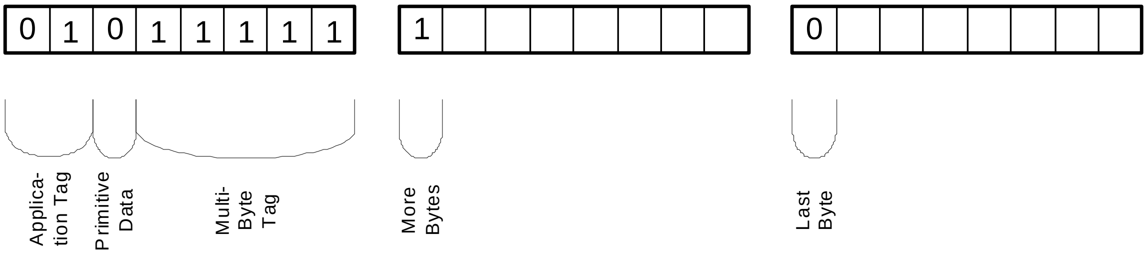

Figure 1: ISO/IEC 8825-2 Coding of a Two-Byte Tag

The high-order bits in the first byte encode the class of the data object. The alternatives are Universal, Application, Context-Specific and Private. All the PIV data objects that appear on the card edge are Application Data objects so ‘01’ is encoded.

The next bit encodes whether the data object is a primitive data object or a constructed data object. Constructed data objects are built up of sub-data objects. Initially, all PIV data objects are treated as primitive data, unstructured sequence-of-bytes data objects at the card edge. While the PIV data model does define a substructure for these data objects, the tags and lengths in these sub-data items do not conform to any standard and in particular to ISO/IEC 8825-2.

The low-order five bits of the first byte can be used to encode one-byte tags but as noted above almost all of these tags have existing meaning in the context of integrated circuit cards. As a result these bits are set to 1 indicating that the tag value itself is encoded in the following bytes.

In each of the following bytes, the high-order bit is set to 1 to indicate that this is NOT the last byte in the sequence of bytes encoding the tag value and the high-order bit is set to 0 to indicate that this byte IS the last byte encoding the tag value.

4.2 BER-TLV Tags in PIV

The two-byte BER-TLV tags used in PIV use the low-order seven bits of the second byte and the low-order seven bits of the third byte to encode the tag value. The allocation of these bits to form a PIV BER-TLV tag is given in Figure 2.

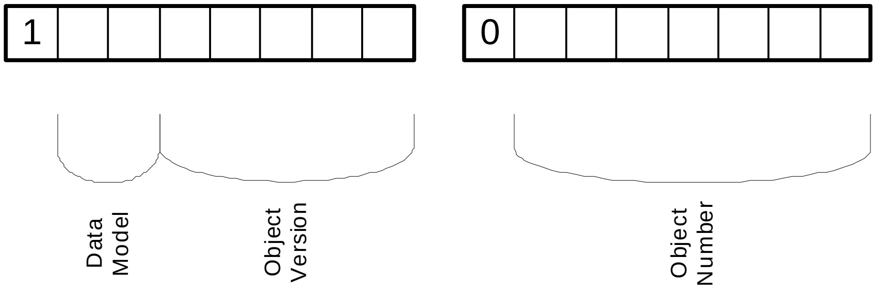

Figure 2: Structure of a Two-Byte PIV BER-TLV Tag

Figure 3 breaks down the encoding of the BER-TLV tag of the CHUID, ‘5F C1 02’, in the initial version of the PIV data model in SP 800-73 dated April 8, 2005.

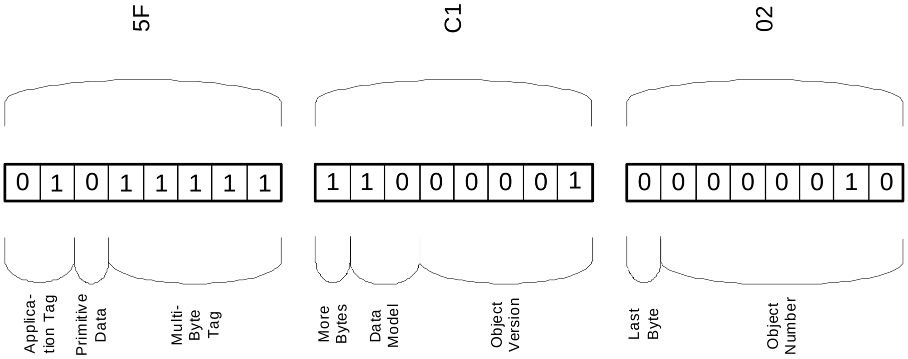

Figure 3: Break-Down of the BER-TLV Tag of the CHUID

5. Key References

This document in combination with SP800-73 will serve as the definitive source for PIV key references. In addition to the key references provided in SP800-73 (Table 12), the following PIV key references are defined:

PIN Unblocking Key: '81'

PIV Card Authentication Key: '9E'

The algorithm identifier associated with the PIV Card Authentication Key may vary as this can be a symmetric or asymmetric key in accordance with SP800-78 and FIPS 201.

6. Non-PIV Data Objects

A PIV card will contain one PIV Card Application as defined in SP800-73 Part 3. The PIV Card Application will support only the PIV data objects defined in PIV standards and specifications maintained by NIST. A PIV card may contain additional card applications, and these applications may or may not choose to conform to the SP800-73 Part 3 card interface. If present, these additional card applications and the data objects they contain are outside the scope of the PIV standards, specifications, and namespaces. However, they should not interfere with the operation of the mandatory PIV card application.